



Data processing device and its method of operation

Patent number: EP1115094
Publication date: 2001-07-11
Inventor: HASS WOLFGANG (DE); WILLE THOMAS DR (DE)
Applicant: PHILIPS CORP INTELLECTUAL PTY (DE); KONINKL
PHILIPS ELECTRONICS NV (NL)

Also published as:

 JP2001230771 (A)
 DE10000503 (A1)

Classification:

- **International:** G07F7/10; G06K19/073
- **European:** G07F7/10D12

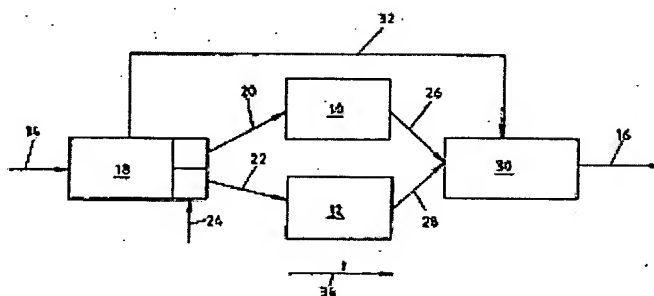
Application number: EP20000204705 20001222

Priority number(s): DE20001000503 20000108

Abstract of EP1115094

During a cryptographic operation in the integrated circuit at least two processors, CPU or co-processors are used in parallel at same time. Single current paths can no longer be reconstructed as current paths of the two parallel operating processors add together, so differential power analysis cannot be used.

Smart card or chip card contains data processing circuitry with CPU or co-processor (10), co-processor (12), with divider (18) between processors and data input (14). Divider divides cryptographic operation into first and second part operations (20,22) with random input (24) to feed data parts to the processors. During the cryptographic operation the two processors operate in parallel at same time. Single current paths can no longer be reconstructed as current paths of the two parallel operating processors add together, so differential power analysis cannot be used.



Data supplied from the *esp@cenet* database - Worldwide

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 1 115 094 A2

(12)

EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
11.07.2001 Patentblatt 2001/28

(51) Int. Cl. 7: G07F 7/10, G06K 19/073

(21) Anmeldenummer: 00204705.8

(22) Anmeldetag: 22.12.2000

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(72) Erfinder:
• Wille, Thomas, Dr., c/o Philips Corporate
52064 Aachen (DE)
• Hass, Wolfgang, c/o Philips Corporate
52064 Aachen (DE)

(30) Priorität: 08.01.2000 DE 10000503

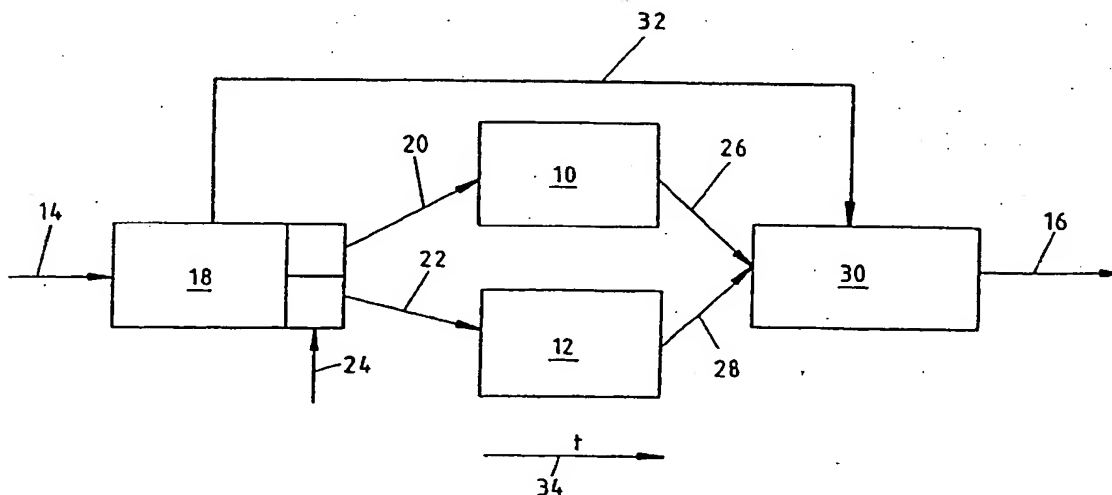
(74) Vertreter: Volmer, Georg, Dipl.-Ing. et al
Philips Corporate Intellectual Property GmbH,
Habsburgerallee 11
52064 Aachen (DE)

(71) Anmelder:
• Philips Corporate Intellectual Property GmbH
52064 Aachen (DE)
Benannte Vertragsstaaten:
DE
• Koninklijke Philips Electronics N.V.
5621 BA Eindhoven (NL)
Benannte Vertragsstaaten:
FR GB

(54) Datenverarbeitungseinrichtung und Verfahren zu dessen Betrieb

(57) Die vorliegende Erfindung betrifft eine Datenverarbeitungseinrichtung, insbesondere Chipkarte oder Smart Card, sowie ein Verfahren zu dessen Betrieb, mit einer integrierten Schaltung, welche eine Zentralschalteneinheit (CPU) (10) sowie einen oder mehrere Co-Prozessor (12) aufweist. Hierbei weist die integrierte

Schaltung eine Steuereinheit (18, 30) auf, welche die Prozessoren, CPU (10) bzw. Co-Prozessoren (12), derart ansteuert, dass im Falle einer kryptographischen Operation wenigstens zwei der Prozessoren gleichzeitig und parallel eine kryptographische Operation ausführen.



EP 1 115 094 A2

Beschreibung

Technisches Gebiet

[0001] Die Erfindung betrifft ein Verfahren zum Betreiben einer Datenverarbeitungseinrichtung, insbesondere einer Chipkarte oder Smart Card, mit einer integrierten Schaltung, welche eine Zentralrecheneinheit (CPU) sowie einen oder mehrere Co-Prozessoren aufweist, wobei von der integrierten Schaltung kryptographische Operationen ausgeführt werden, gemäß dem Oberbegriff des Anspruchs 1. Die Erfindung betrifft ferner eine Datenverarbeitungseinrichtung, insbesondere Chipkarte oder Smart Card, mit einer integrierten Schaltung, welche eine Zentralrecheneinheit (CPU) sowie einen oder mehrere Co-Prozessor aufweist, gemäß dem Oberbegriff des Anspruchs 10.

Stand der Technik

[0002] In vielen Datenverarbeitungsgeräten mit integrierter Schaltung dienen beispielsweise kryptographische Operationen zum Schutz des Betriebes dieser Geräte bzw. zum Schutz von in dem Gerät gespeicherten Daten. Die hierfür notwendigen Rechenoperationen werden dabei sowohl von Standard-Rechenwerken (CPU) als auch von dedizierten Crypto-Rechenwerken (Co-Prozessor) durchgeführt. Ein typisches Beispiel für letzteres sind Chipkarten bzw. IC-Karten, wie beispielsweise eine sogen. Smart Card. Bei in diesem Zusammenhang verwendeten Daten bzw. Zwischenergebnissen handelt es sich üblicherweise um sicherheitsrelevante Informationen, wie beispielsweise kryptographische Schlüssel oder Operanden.

[0003] Bei von der integrierten Schaltung durchgeführten Rechenoperationen, beispielsweise zur Berechnung von kryptographischen Algorithmen, werden logische Verknüpfungen zwischen Operanden bzw. Zwischenergebnissen durchgeführt. In Abhängigkeit von der verwendeten Technologie führen diese Operationen, insbesondere das Laden von leeren oder zuvor gelöschten Speicherbereichen bzw. Register mit Daten, zu einem erhöhten Stromverbrauch der Datenverarbeitungsgeräte. Bei komplementärer Logik, wie beispielsweise der CMOS-Technik, tritt ein erhöhter Stromverbrauch dann auf, wenn der Wert einer Bit-Speicherzelle geändert wird, d.h. sein Wert sich von "0" auf "1" ändert. Der erhöhte Verbrauch hängt dabei von der Anzahl der im Speicher bzw. Register geänderten Bitstellen ab. Mit anderen Worten lässt das Laden eines zuvor gelöschten Registers einen Stromverbrauch proportional zum Hamminggewicht des in das leere Register geschriebenen Operanden (=Anzahl der Bits mit dem Wert "1") ansteigen. Durch eine entsprechende Analyse dieser Stromänderung könnte es möglich sein, Informationen über die berechneten Operationen zu extrahieren, so dass eine erfolgreiche Kryptoanalyse von geheimen Operanden, wie beispielsweise kryptographischen Schlüsseln,

möglich ist. Mittels Durchführung mehrerer Strommessungen am Datenverarbeitungsgerät könnte beispielsweise bei sehr kleinen Signaländerungen eine hinreichende Extraktion der Informationen ermöglicht werden. Andererseits könnten mehrere Strommessungen eine ggf. erforderliche Differenzbildung ermöglichen. Diese Art der Kryptoanalyse wird auch als "Differential Power Analysis" bezeichnet, mittels derer ein Außenstehender durch reine Beobachtung von Änderungen des Stromverbrauches des Datenverarbeitungsgerätes eine ggf. unberechtigte Kryptoanalyse der kryptographischen Operationen, Operanden bzw. Daten erfolgreich ausführen kann. Die "Differential Power Analysis" ermöglicht somit über eine reine Funktionalität hinaus zusätzliche interne Informationen einer integrierten Schaltung gewinnen zu können.

[0004] Ein typisches Einsatzgebiet von den vorerwähnten Smart Cards sind beispielsweise Applikationen, bei denen die Smart Card als sicherer Informationsspeicher benutzt wird. Kryptographische Operationen sichern dabei den Zugang zu diesen Applikationen, indem die Smart Card selbständig Verschlüsselungsoperationen zum Zwecke der Authentikation ausführt. Dies ist nur möglich durch Verwendung eines speziellen Smart Card Controllers (Mikrocontrollers), der durch geeignete Software gesteuert wird. Der Kommunikationskanal zwischen Smart Card Controller und Smart Card Terminal ist direkt durch kryptographische Methoden gesichert, deren Sicherheitsniveau wesentlich vom verwendeten kryptographischen Algorithmus abhängt.

[0005] Um den Authentikationsvorgang einer Smart Card fälschen zu können, muss das Authentikationsprotokoll mittels eines Nachbaus emuliert werden können. Dies ist bei sicheren Protokollen nur dadurch möglich, indem der verwendete geheime kryptographische Schlüssel analysiert wird, der auf der Smart Card gespeichert ist.

[0006] Da Smart Card Controller reproduzierbar arbeitende Maschinen sind, könnten mittels der Analyse von indirekten Abstrahlungen einer Smart Card während der Operation, etwa durch Messen des zeitlichen Verlaufs des Stromverbrauchs mit der o.g. "Differential Power Analysis", interne Vorgänge im Smart Card Controller bestimmt und letztendlich der geheime Schlüssel ermittelt werden. Analysiert wird hierbei das reproduzierbare, deterministische Stromprofil für gleiche Programmsequenzen einer Smart Card Controllerschaltung.

[0007] Aus der US 4 813 024 ist eine integrierte Schaltung zum Speichern und Verarbeiten geheimer Daten bekannt, wobei ein Speicher eine Simulationsspeicherzelle aufweist, welche einen identischen Stromverbrauch aufweist wie eine Speicherzelle, die bisher nicht programmiert wurde. Hierdurch werden Schwankungen in Strom und Spannung nur für die Speicherzelle eliminiert, jedoch nicht für die Verarbeitung der Daten.

Bester Weg zur Ausführung der Erfindung

[0024] Die einzige Figur zeigt einen Teil einer integrierten Schaltung einer ansonsten nicht näher dargestellten Datenverarbeitungseinrichtung, welche beispielsweise eine Smart Card oder eine Chipkarte ist. Die integrierte Schaltung umfasst eine zentrale Recheneinheit (CPU) oder einen Co-Prozessor A 10, einen Co-Prozessor B 12, einen Dateneingang 14 und einen Datenausgang 16. Zwischen dem Dateneingang 14 und der CPU oder einem Co-Prozessor A 10 bzw. dem Co-Prozessor B 12 ist ein Aufteiler 18 angeordnet, welcher im Falle einer von der integrierten Schaltung auszuführenden kryptographischen Operation diese in eine erste und zweite Teiloperation in Form eines ersten Datenteils 20 und eines zweiten Datenteils 22 aufteilt. Der erste Datenteil 20 wird der CPU oder dem Co-Prozessor A 10 und der zweite Datenteil 22 wird dem Co-Prozessor B 12 zum Abarbeiten mittels einer vorbestimmten kryptographischen Operation zugeführt. Der Aufteiler 18 weist ferner einen Zufallseingang 24 auf, mittels dem die Aufteilung in die Datenteile 20, 22 zufallsgesteuert ausgeführt wird.

[0025] Die CPU oder der Co-Prozessor A 10 und der Co-Prozessor B 12 führen eine jeweilige kryptographische Operation gleichzeitig und parallel aus. Hierdurch überlagern sich entsprechende Stromverbrauchskurven (Stromverbrauchsamplitude über Zeit), so dass die Einzelkurven der Einzelgeräte 10, 12 bzw. der jeweils in den Prozessoren 10, 12 getrennt ablaufenden Einzelprozesse nicht mehr analysiert werden können.

[0026] Aus der CPU oder dem Co-Prozessor A 10 kommt ein erstes Ergebnis 26 und aus dem Co-Prozessor B 12 kommt ein zweites Ergebnis 28, welche in einem Rekombinierer 30 wieder zu einem Gesamtergebnis zusammen gefasst und dem Datenausgang 16 zugeführt werden. Über eine Verbindung 32 informiert dabei der Aufteiler 18 den Rekombinierer 30 darüber, wie die jeweiligen Teilergebnisse 26, 28 wieder zusammen zu fügen sind. Dies ist notwendig, da aufgrund des Zufallseingangs 24 die Aufteilung durch den Aufteiler 18 immer in zufällig unterschiedlicher Weise erfolgt.

[0027] Ein Pfeil bzw. eine Zeitachse 34 veranschaulicht den Datenfluss durch die erfindungsgemäße Vorrichtung über die Zeit. Die Daten gelangen am Dateneingang 14 in der Fig. links in die Vorrichtung, gelangen über zwei parallele Datenwege 20, 22 zu den Prozessoren 10, 12, werden in den Prozessoren 10, 12 weiterverarbeitet und gelangen über die Wege 26, 28 wieder zusammen und verlassen die Vorrichtung in der Fig. rechts über den Datenausgang 16. Diese Daten umfassen beispielsweise an der Seite des Dateneingangs 14 einen kryptographischen Schlüssel oder Operanden, welcher zur Authentikation in den Prozessoren 10, 12 eine kryptographische Operation durchlaufen, wobei eine Authentikation nur dann als erfolgreich bzw. positiv angesehen wird, wenn am Datenausgang 16 ein vorbestimmtes Ergebnis ankommt.

[0028] Zur Verschleierung des sich aufgrund der kryptographischen Operation ergebenden zeitlichen Schwankungen des Stromverbrauchs, welche in der sogenannten "Differential Power Analysis" einen Rückschluss auf die kryptographische Operation bzw. den richtigen kryptographischen Schlüssel erlauben könnte, werden die Prozessoren von der aus Aufteiler 18 und Rekombinierer 30 gebildeten Steuereinheit derart angesteuert, dass die beiden Prozessoren 10, 12 gleichzeitig und parallel eine kryptographische Operation ausführen, so dass sich deren Stromverbrauchskurven überlagern und nicht mehr getrennt analysiert werden können. Mit anderen Worten ist eine Trennung des von außen messbaren zeitlichen Verlaufes des Gesamtstromes nicht mehr möglich.

[0029] Hierbei wird der Schlüssel beispielsweise in zwei Datenteile 20, 22 aufgeteilt, welche jeweils getrennt voneinander in den Prozessoren 10, 12 einer kryptographischen Operation unterzogen und die Einzelergebnisse wieder zusammen geführt werden. Alternativ läuft in beiden Prozessoren 10, 12 exakt dieselbe kryptographische Operation ab, jedoch erhält nur ein Prozessor 10 oder 12, beispielsweise die CPU oder der Co-Prozessor A 10, den richtigen Schlüssel, während der jeweils andere Prozessor, beispielsweise der Co-Prozessor B 12, einen falschen Schlüssel erhält. Über die Verbindung 32 informiert der Aufteiler 18 den Rekombinierer 30, dass dieser das zweite Ergebnis 29 zu verwerfen hat und lediglich das erste Ergebnis 26 aus der CPU oder dem Co-Prozessor A 10 an den Datenausgang 16 übergibt. Ist hierbei der dem Co-Prozessor B 12 zugeführte falsche Schlüssel das Komplement des der CPU oder dem Co-Prozessor A 10 zugeführten echten Schlüssel, so ergeben sich bei der Ausführung der kryptographischen Operation komplementäre Stromverbrauchswerte in den beiden Prozessoren 10, 12, welche eine "Differential Power Analysis" faktisch unmöglich machen.

[0030] Es erfolgt die Aufteilung der kryptographischen Operation auf die beiden Prozessoren 10, 12 derart, dass niemals die typischen Stromverbrauchsverläufe der kryptographischen Operation eines einzelnen Schaltungsteiles 10, 12 ohne parallele Operation des jeweils anderen Schaltungsteils 10, 12, also CPU oder Co-Prozessor A 10 bzw. Co-Prozessor B 12, sichtbar werden.

[0031] Die Steuereinheit 18, 30 nimmt die Aufteilung in Teilaufgaben beispielsweise derart vor, dass durch Zufall gesteuert entschieden wird, welcher Schaltungsteil 10, 12 die relevante kryptographische Operation ausführt. Der zu dem Zeitpunkt nicht relevante Schaltungsteil 10, 12 führt parallel dazu eine geeignete kryptographische Operation (Dummyoperation) aus, die sich im Stromverlauf völlig gleichwertig abbildet, aber für die Gesamtberechnung unerheblich ist.

[0032] Beispielsweise werden Teile einer DES (Data Encryption Standard) Verschlüsselung kontinuierlich oder auch nur teilweise die linke oder rechte Teilver-

Darstellung der Erfindung, Aufgabe, Lösung, Vorteile

[0008] Es ist Aufgabe der vorliegenden Erfindung, ein verbessertes Verfahren sowie eine verbesserte Datenverarbeitungseinrichtung der obengenannten Art zur Verfügung zu stellen, welche die obengenannten Nachteile beseitigen und eine "Differential Power Analysis" so weit wie möglich erschweren.

[0009] Diese Aufgabe wird durch ein Verfahren der o. g. Art mit den in Anspruch 1 gekennzeichneten Merkmalen und durch eine Datenverarbeitungseinrichtung der o. g. Art mit den in Anspruch 10 gekennzeichneten Merkmalen gelöst.

[0010] Dazu ist es bei einem Verfahren der o. g. Art erfindungsgemäß vorgesehen, dass bei Durchführung einer kryptographischen Operation in der integrierten Schaltung jeweils wenigstens zwei Prozessoren, CPU bzw. Co-Prozessoren, gleichzeitig und parallel eine kryptographische Operation ausführen.

[0011] Dies hat den Vorteil, dass sich im Betrieb während einer kryptographischen Operation ein Stromverbrauch der Datenverarbeitungseinrichtung aus den jeweiligen Stromaufnahmen der wenigstens zwei parallel arbeitenden Prozessoren aufsummiert, so dass die einzelnen Stromverläufe nicht mehr rekonstruierbar sind. Eine "Differential Power Analysis" ist somit nicht mehr erfolgreich durchführbar.

[0012] Vorzugsweise Weitergestaltungen des Verfahrens sind in den Ansprüchen 2 bis 9 beschrieben.

[0013] In einer bevorzugten Ausführungsform ist nur die kryptographische Operation eines Prozessors, CPU bzw. Co-Prozessoren, eine Nutzoperation und sind alle anderen kryptographischen Operationen Dummyoperationen, deren Ergebnis verworfen wird, wobei optional die Auswahl, welcher Prozessor, CPU oder Co-Prozessor, eine Nutzoperation ausführt, zufallsgesteuert wird.

[0014] In einer alternativen bevorzugten Ausführungsform ist die kryptographische Operation im Sinne des Stromverbrauchs aufgeteilt in zwei zueinander komplementäre Operationen. Führen nun zwei identische Co-Prozessoren die jeweils komplementäre kryptographische Operation zeitgleich aus, addieren sich die Stromverläufe ebenfalls komplementär, so dass eine DPA nicht mehr erfolgreich durchgeführt werden kann bzw. im Aufwand erheblich gesteigert werden muss.

[0015] Zum Erzielen einer besonders starken Verschleierung der von der "Differential Power Analysis" verwendeten Stromkurve und um etwaige Asymmetrien in den identisch konstruierten Co-Prozessoren auszugleichen, wird die kryptographische Operation in Teiloperationen zerlegt. Die Auswahl, welcher Co-Prozessor welche Operation komplementär oder nicht-komplementär ausführt wird dabei zufallsgesteuert.

[0016] In einer weiteren alternativen Ausführungsform wird eine kryptographische Operation in wenigstens zwei Teiloperationen aufgeteilt und werden die Teiloperationen gleichzeitig und parallel von den Pro-

zessoren, CPU bzw. Co-Prozessoren, ausgeführt sowie anschließend entsprechende Teilergebnisse zu einem Gesamtergebnis der gesamten kryptographischen Operation zusammengefügt. Optional wird die Aufteilung der kryptographischen Operation in Teiloperationen zufallsgesteuert. Beispielsweise sind die Teiloperationen Teile einer Verschlüsselung nach DES (Data Encryption Standard).

[0017] Ferner ist es bei einer Datenverarbeitungseinrichtung erfindungsgemäß vorgesehen, dass die integrierte Schaltung eine Steuereinheit aufweist, welche die Prozessoren, CPU bzw. Co-Prozessoren, derart ansteuert, dass im Falle einer kryptographischen Operation wenigstens zwei der Prozessoren gleichzeitig und parallel eine kryptographische Operation ausführen.

[0018] Dies hat den Vorteil, dass sich im Betrieb während einer kryptographischen Operation ein Stromverbrauch der Datenverarbeitungseinrichtung aus den jeweiligen Stromaufnahmen der wenigstens zwei parallel arbeitenden Prozessoren aufsummiert, so dass die einzelnen Stromverläufe nicht mehr rekonstruierbar sind. Eine "Differential Power Analysis" ist somit nicht mehr erfolgreich durchführbar.

[0019] Vorzugsweise Weiterbildungen der Datenverarbeitungseinrichtung sind in den Ansprüchen 11 bis 14 beschrieben.

[0020] In einer bevorzugten Ausführungsform weist die Steuereinheit einen Aufteiler auf, welcher eine kryptographische Operation in wenigstens zwei Teiloperationen aufteilt und zur gleichzeitigen Abarbeitung an zwei getrennte Prozessoren der integrierten Schaltung, CPU bzw. Co-Prozessoren, zuführt, wobei die Steuereinheit bevorzugt ferner einen Rekombinierer aufweist, welcher jeweilige Teilergebnisse aus den von den Prozessoren gleichzeitig ausgeführten Teiloperationen wieder zusammenführt.

[0021] Zum Verhindern einer erfolgreichen Analyse einer Stromverbrauchskurve während der kryptographischen Operation ist der Aufteiler derart ausgebildet, dass wenigstens eine Teiloperation eine Dummyoperation ist, und dass der Rekombinierer derart ausgebildet ist, dass dieser das jeweilige Ergebnis aus einem Prozessor, welcher eine Dummyoperation ausgeführt hat, verwirft.

[0022] Eine besonders gute Verschleierung der Stromverbrauchskurve erzielt man dadurch, dass die integrierte Schaltung zusätzlich einen Zufallsgenerator aufweist, welcher derart mit dem Aufteiler verbunden ist, dass dieser zufallsgesteuert arbeitet.

Kurze Beschreibung der Zeichnungen

[0023] Nachstehend wird die Erfindung anhand der beigefügten Zeichnung näher erläutert. Diese zeigt in der einzigen Fig. ein schematisches Blockschaltbild eines Teils einer integrierten Schaltung einer erfindungsgemäßen Datenverarbeitungseinrichtung.

schlüsselung auf beide Schaltungsteile 10, 12 in durch Zufall ausgewählten Runden ausgetauscht.

[0033] Alternativ werden bei der Berechnung eines Triple-DES (einer mehrstufigen Verschlüsselung) die jeweils relevanten DES-Operationen zufällig zwischen den beiden Schaltungsteilen 10 und 12 verteilt, so dass nie vorhersehbar ist, welcher Schaltungsteile 10 oder 12 gerade die relevante kryptographische Operation ausführt. Bei der Steuerung beider Schaltungsteile 10, 12 ist zu beachten, dass deren typisches Frequenzspektrum zumindest in Teilen identisch ist, so dass sich Überlagerungen beider Stromverbrauchsprofile auch nicht im Frequenzraum mittels einer Fourier-Transformation separieren lassen.

BEZUGSZEICHENLISTE

[0034]

- 10 zentrale Recheneinheit (CPU)
- 12 Co-Prozessor
- 14 Dateneingang
- 16 Datenausgang
- 18 Aufteiler
- 20 erster Datenteil
- 22 zweiter Datenteil
- 24 Zufallseingang
- 26 erstes Ergebnis
- 28 zweites Ergebnis
- 30 Rekombinierer
- 32 Verbindung zw. Aufteiler und Rekombinierer
- 34 Zeitachse

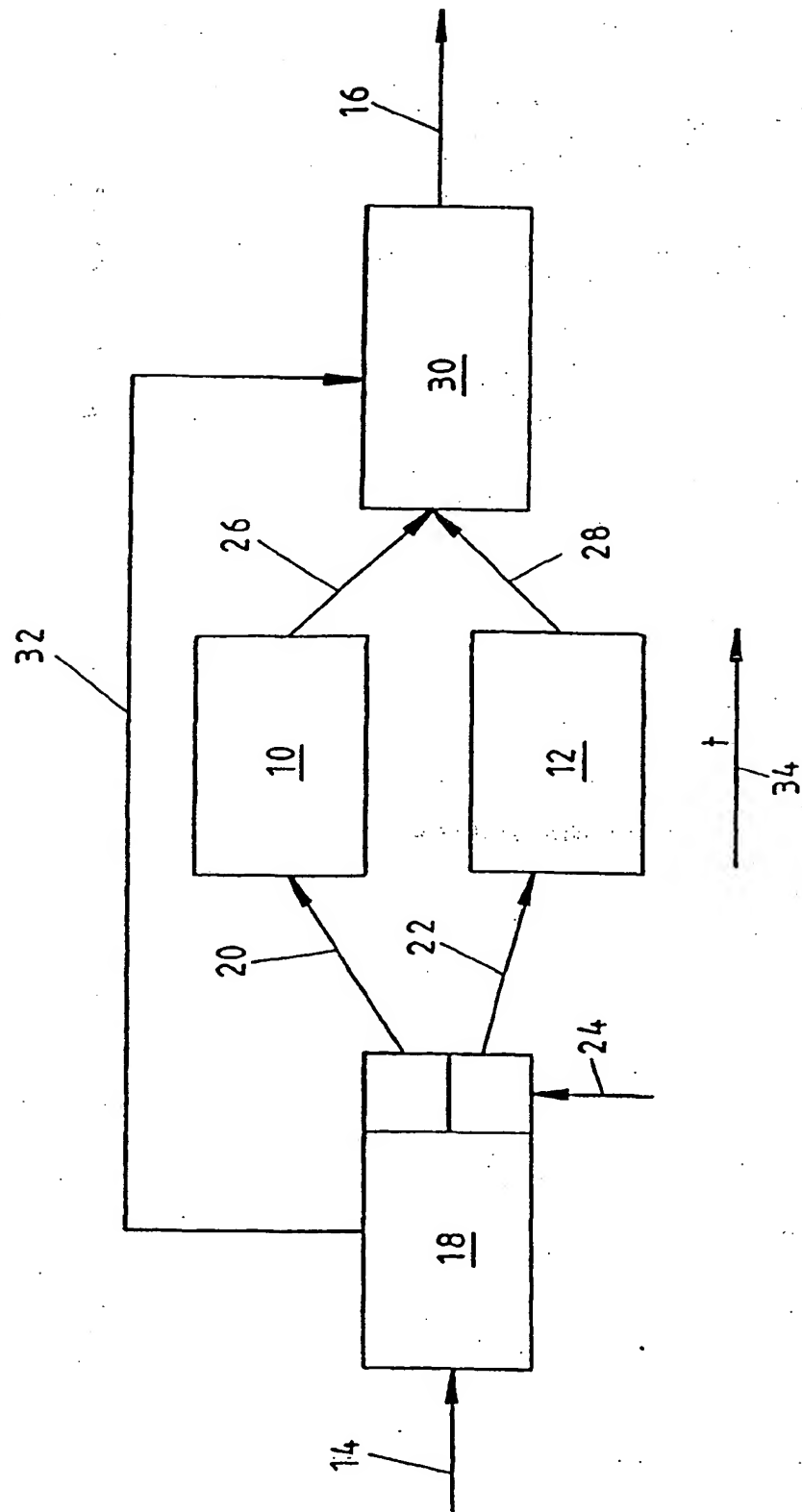
Patentansprüche

1. Verfahren zum Betreiben einer Datenverarbeitungseinrichtung, insbesondere einer Chipkarte oder Smart Card, mit einer integrierten Schaltung, welche eine Zentralrecheneinheit (CPU) sowie einen oder mehrere Co-Prozessoren aufweist, wobei von der integrierten Schaltung kryptographische Operationen ausgeführt werden, dadurch gekennzeichnet, dass bei Durchführung einer kryptographischen Operation in der integrierten Schaltung jeweils wenigstens zwei Prozessoren, CPU bzw. Co-Prozessoren, gleichzeitig und parallel eine kryptographische Operation ausführen.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass nur die kryptographische Operation eines Prozessors, CPU bzw. Co-Prozessoren, eine Nutzoperation und alle anderen kryptographischen Operationen Dummyoperationen sind, deren Ergebnis verworfen wird.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Auswahl, welcher Prozessor, CPU oder Co-Prozessoren, eine Nutzoperation ausführt, zufallsgesteuert wird.
4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass eine kryptographische Operation in wenigstens zwei Teiloperationen zerlegt wird und wenigstens zwei Prozessoren diese Teiloperationen parallel zeitgleich ausführen.
5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass eine kryptographische Operation im Sinne des Stromverbrauchs in zwei zueinander komplementäre Operationen aufgeteilt wird.
6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass die Auswahl, welcher Prozessor die Operation komplementär oder nicht-komplementär ausführt zufallsgesteuert wird.
7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass eine kryptographische Operation in wenigstens zwei Teiloperationen aufgeteilt und die Teiloperationen gleichzeitig und parallel von den Prozessoren, CPU bzw. Co-Prozessoren, ausgeführt werden sowie anschließend entsprechende Teilergebnisse zu einem Gesamtergebnis der gesamten kryptographischen Operation zusammengefügt werden.
8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass die Aufteilung der kryptographischen Operation in Teiloperationen zufallsgesteuert wird.
9. Verfahren nach Anspruch 7 oder 8, dadurch gekennzeichnet, dass die Teiloperationen Teile einer Verschlüsselung nach DES (Data Encryption Standard) sind.
10. Datenverarbeitungseinrichtung, insbesondere Chipkarte oder Smart Card, insbesondere zum Ausführen eines Verfahrens gemäß wenigstens einem der vorhergehenden Ansprüche, mit einer integrierten Schaltung, welche eine Zentralrecheneinheit (CPU) (10) sowie einen oder mehrere Co-Prozessoren (12) aufweist, dadurch gekennzeichnet, dass die integrierte Schaltung eine Steuereinheit (18, 30) aufweist, welche die Prozessoren, CPU (10) bzw. Co-Prozessoren (12), derart ansteuert,

dass im Falle einer kryptographischen Operation wenigstens zwei der Prozessoren gleichzeitig und parallel eine kryptographische Operation ausführen.

- 5
11. Datenverarbeitungseinrichtung nach Anspruch 10,
dadurch gekennzeichnet,
dass die Steuereinheit einen Aufteiler (18) aufweist,
welcher eine kryptographische Operation in wenig-
stens zwei Teiloperationen (20, 22) aufteilt und zur
gleichzeitigen Abarbeitung an zwei getrennte Pro-
zessoren der integrierten Schaltung, CPU (10) bzw.
Co-Prozessoren (12), zuführt. 10
12. Datenverarbeitungseinrichtung nach Anspruch 11, 15
dadurch gekennzeichnet,
dass die Steuereinheit ferner einen Rekombinierer
(30) aufweist, welcher jeweilige Teilergebnisse (26,
28) aus den von den Prozessoren (10, 12) gleich-
zeitig ausgeführten Teiloperationen (20, 22) wieder 20
zusammenführt.
13. Datenverarbeitungseinrichtung nach Anspruch 12,
dadurch gekennzeichnet,
dass der Aufteiler (18) derart ausgebildet ist, dass 25
wenigstens eine Teiloperation (20, 22) eine Dum-
myoperation ist, und dass der Rekombinierer (30)
derart ausgebildet ist, dass dieser das jeweilige Er-
gebnis (26, 28) aus einem Prozessor (10, 12), wel-
cher eine Dummyoperation ausgeführt hat, verwirft. 30
14. Datenverarbeitungseinrichtung nach einem der An-
sprüche 11 bis 13,
dadurch gekennzeichnet,
dass die integrierte Schaltung zusätzlich einen Zu-
fallsgenerator (24) aufweist, welcher derart mit dem 35
Aufteiler (18) verbunden ist, dass dieser zufallsge-
steuert arbeitet.
- 40
- 45
- 50
- 55





DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁷ : G06F 1/00		(11) Numéro de publication internationale: WO 00/39660
A1		(43) Date de publication internationale: 6 juillet 2000 (06.07.00)
(21) Numéro de la demande internationale: PCT/FR99/03275 (22) Date de dépôt international: 23 décembre 1999 (23.12.99) (30) Données relatives à la priorité: 98/16485 28 décembre 1998 (28.12.98) FR (71) Déposant (pour tous les Etats désignés sauf US): BULL CP8 [FR/FR]; 68, route de Versailles, Boite postale 45, F-78430 Louvécienne (FR). (72) Inventeurs; et (75) Inventeurs/Déposants (US seulement): GRESSUS, Yvon [FR/FR]; 39, rue Pasteur, F-78340 Les Clayes sous Bois (FR). SIEGELIN, Christoph [DE/FR]; 32, rue Ginoux, F-75015 Paris (FR). UGON, Michel [FR/FR]; 6, rue des Cépages, F-78310 Maurepas (FR). (74) Mandataire: BULL S.A.; Coriu, Bernard , 68, route de Versailles, PC58D20, F-78434 Louvecienne Cedex (FR).		(81) Etats désignés: BR, CN, JP, KR, SG, US , brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Publiée Avec rapport de recherche internationale.

(54) Title: SMART INTEGRATED CIRCUIT

(54) Titre: CIRCUIT INTEGRE INTELLIGENT

(57) Abstract

The invention concerns a smart integrated circuit characterised in that it has a main processor (1) and an operating system executing a main programme (P1) to set up a main process performing tasks, at least a secondary processor (2) capable of executing simultaneously at least a secondary programme (P2) to constitute a task-performing process, power circuits (6) common to the processors and means ensuring that the secondary process(es) with similar energy and different operating signature, are carried out simultaneously with the main process by inducing in the power circuits, continuously or intermittently, energy disturbances which are superposed on those of the main process to produce continuous or intermittent data encryption.

(57) Abrégé

La présente invention concerne un circuit intégré intelligent. Ce circuit intégré intelligent est caractérisé en ce qu'il possède un processeur principal (1) et un système d'exploitation exécutant un programme principal (P1) pour constituer un processus principal réalisant des tâches, au moins un processeur secondaire (2) capable d'exécuter concurrentiellement au moins un programme secondaire (P2) pour constituer au moins un processus réalisant des tâches, des circuits d'alimentation (6) communs entre les processeurs et des moyens permettant de s'assurer que le ou les processus secondaires d'énergie similaire et de signature de fonctionnement différente, s'effectuent concurrentiellement avec le processus principal en induisant dans les circuits d'alimentation, de façon continue ou intermittente, des perturbations énergétiques qui se superposent à celle du processus principal pour réaliser un brouillage continu ou intermittent.

